ON-LINE PIN VERIFICATION USING POLYNOMIALS

W. Dale Hopkins

ABSTRACT

A technique for on-line Personal Identification Number (PIN) verification uses polynomial hiding. The technique comprises enrolling a smart card, including initializing a smart card with an entity-selected PIN hidden in a polynomial over a finite field. The initialization polynomial is a function of the PIN, an entity-identifier, and a random number. The random number and the PIN are discarded after smart card initialization.